

Balík nástrojov Microsoft Sysinternals

Marek Čederle

Fakulta informatiky a informačných technológií

Slovenská Technická Univerzita v Bratislave

Bratislava, Slovensko

xcederlem@stuba.sk

Abstrakt—Táto práca sa zaobráva analýzou a experimentovaním s bezpečnostnými nástrojmi z balíka Microsoft Sysinternals. Tento balík obsahuje široké spektrum nástrojov určených na správu, diagnostiku a monitorovanie operačného systému Microsoft Windows, s dôrazom na bezpečnosť. Práca sa sústredí na vybrané nástroje, konkrétnie Process Explorer, Autoruns, TCPView a Process Monitor, pričom každý z nich bol použitý pri testovaní reálnych vzoriek malvér. V rámci experimentov bola využitá cloudrová virtuálna infraštruktúra pre zabezpečenie bezpečného prostredia na spúšťanie malvér. Cieľom práce bolo demonštrovať funkcie týchto nástrojov pri detekcii a analýze škodlivých aktivít. Výsledky ukázali, že nástroje z balíka Sysinternals poskytujú robustné možnosti pre monitoring a analýzu systémových procesov a sú užitočným doplnkom v oblasti kybernetickej bezpečnosti.

Kľúčové slová—Sysinternals, Microsoft, Windows, malvér, kybernetická bezpečnosť, virtuálny stroj, Process Explorer, Process Monitor, Autoruns, TCPView

I. FUNKČNÝ OPIS BEZPEČNOSTNÉHO NÁSTROJA

A. Úvod do Microsoft Sysinternals

Windows Sysinternals je balík nástrojov, ktorý sa zameriava na správu, diagnostiku, riešenie problémov a monitorovanie operačného systému MS¹ Windows. Pôvodne Sysinternals bola webová stránka (predtým známa ako ntinternals) vytvorená v roku 1996 a prevádzkovala ju spoločnosť Winternals Software LP so sídlom v Austine v Texase. Založili ju softvéroví vývojári Bryce Cogswell a Mark Russinovich. 18. júla 2006 spoločnosť Winternals bola zakúpená spoločnosťou Microsoft.

Webová stránka obsahovala niekoľko freewarových nástrojov na správu a monitorovanie počítačov s operačným systémom MS Windows. Spoločnosť predávala aj nástroje na obnovu dát a profesionálne edície svojich freewarových nástrojov [1]. Aktuálny zoznam nástrojov [2] je zobrazený v Tabuľke č. I.

B. Prehľad vybraných nástrojov

Pre účely tohto projektu sme sa zamerali iba na päť vybraných nástrojov z balíku nástrojov Sysinternals, ktoré sú zamerané na bezpečnosť alebo majú uplatnenie v tejto oblasti. Je to predovšetkým kvôli tomu, že Sysinternals obsahuje nesmierne veľa rôznych nástrojov a bolo by to mimo rozsahu a zamerania tejto práce v predmete PRBIT².

TABUĽKA I: ZOZNAM NÁSTROJOV BALÍKA SYSINTERNALS

AccessChk	Junction	PsService
AccessEnum	LDMDump	PsShutdown
AdExplorer	ListDLLs	PsSuspend
AdInsight	LiveKd	PsTools
AdRestore	LoadOrder	RAMMap
Autologon	LogonSessions	RDCMan
Autoruns	MoveFile	RegDeleteNull
BgInfo	NotMyFault	RegHide
BlueScreen	NTFSInfo	RegJump
CacheSet	PendMoves	Registry Usage (RU)
ClockRes	PipeList	SDelete
Contig	PortMon	ShareEnum
Coreinfo	ProcDump	ShellRunas
Ctrl2Cap	Process Explorer	Sigcheck
DebugView	Process Monitor	Streams
Desktops	PsExec	Strings
Disk2vhd	PsFile	Sync
DiskExt	PsGetSid	Sysmon
DiskMon	PsInfo	TCPView
DiskView	PsKill	VMMAP
Disk Usage (DU)	PsList	VolumeID
EFDSDump	PsLoggedOn	WhoIs
FindLinks	PsLogList	WinObj
Handle	PsPasswd	ZoomIt
Hex2dec	PsPing	—

1) **Process Explorer**: Process explorer je nástroj, ktorý má veľmi podobné funkcionality ako klasický Task Manager³, ktorý je vstavaný v každom operačnom systéme MS Windows už od verzie Windows NT 4.0. Vie zobraziť využite CPU⁴ procesmi na danom systéme. Taktiež využitie operačnej pamäte jednotlivými procesmi, ich PID⁵ a popis. Jeho výhodou je, že je veľmi podrobnej oproti jednoduchému Správcovi úloh, hlavne čo sa týka informácií ohľadom správy pamäte. Niektorí ľudia ho nazývajú aj „Task Manager na steroidoch“ alebo „Super Task Manager“. Zobrazuje procesy v tzv. stromovej štruktúre čo znamená, že je jednoducho vidieť, ktorý proces spustil iný proces (resp. ktorý proces je rodičom ďalších procesov). Po kliknutí na vybraný proces, program dokáže zobraziť vlákna⁶ daného procesu a dynamické knižnice⁷, ktoré používa. Po otvorení vlastnosti jednotlivého procesu nám vyskočí okno,

³Správca úloh

⁴procesora

⁵Process ID

⁶threads

⁷DLL — Dynamic-Link Library

¹Microsoft

²Princípy bezpečnosti v informačných technológiách

kde sú všetky podrobnosti, ktoré sa vôbec o procese v rámci operačného systému dajú získať. Nástroj obsahuje aj vyhľadávanie procesov, čo bola funkcia, ktorú napríklad Správca úloh získal až vo verzii Windows 11. Ďalšou funkciou Process Explorera je aj možnosť zobraziť informácie o sieťových pripojeniach, ktoré daný proces vytvára. Taktiež dokáže zobraziť bezpečnostné politiky, ktoré boli aplikované na daný proces. V neposlednom rade tento nástroj vie poslať vzorku daného procesu (programu) na webovú stránku [VirusTotal.com](https://www.virustotal.com), ktorá slúži na skenovanie potenciálne škodlivého softvéru⁸. Nástroj dokáže overiť signatúry ostatných spustených programov, t.z. či je daný program podpísaný oficiálnym certifikátom spoločnosti, ktorá ho vyvíja. Samozrejmostou je spomenút aj veľmi užitočnú funkciu nástroja, ktorú vieme vyvolať kliknutím na ikonu „mieridla“ v hlavnom menu, ktorá pri kliknutí na hocjaké okno vie identifikovať proces, ktorému dané okno patrí, čo môže byť užitočné napríklad pri systéme, na ktorom sa nachádza Adware.

2) *AutoRuns*: Nástroj Autoruns slúži na správu programov, ktoré sa spúšťajú pri štarte systému⁹. Taktiež ako predošlý nástroj, aj nástroj Autoruns vie odoslať vzorky na webovú stránku [VirusTotal.com](https://www.virustotal.com), aby overil, či dané programy sú škodlivé a vie overiť aj signatúry programov. Tento nástroj vie zobraziť veľa rôznych kategórií, ktoré označujú ako, kedy a akým spôsobom sa spúšťa daný program pri štarte operačného systému. Najzaujímavejšie kategórie sú:

- **Logon:** Programy, spúšťajúce sa po prihlásení používateľa na daný systém.
- **Explorer:** Doplňky a rozšírenia „shellu“ pre prieskumník systému Windows. Môžu zahŕňať položky kontextovej ponuky (ponuka vyvolaná po kliknutí pravým tlačidlom) a iné rozšírenia.
- **Scheduled Tasks:** Programy nastavené na spúšťanie pomocou Plánovača úloh¹⁰ systému Windows. Tieto programy sa spúšťajú na nejakú akciu (trigger) čo môže byť napríklad čas.
- **Services:** Služby systému Windows, ktoré sa spúšťajú na pozadí. Môžu byť nastavené na spúšťanie spolu so systémom, s oneskorením alebo manuálne.
- **Drivers:** Ovládače, ktoré sa načítajú počas spúšťania systému.

V každej kategórii sa nachádzajú klúče registrov, kde sú dané informácie uložené. Môžu sa však nachádzať aj v súborovom systéme, napríklad ak si vytvoríme vlastný odkaz na aplikáciu, ktorá sa ma zapnúť pri spustení systému¹¹.

3) *TCPView*: Nástroj TCPView slúži na monitorovanie sieťovej aktivity. Nie je to však tak komplexný nástroj ako napríklad Wireshark, ktorý vie zachytávať priamo packety a celú sieťovú komunikáciu daného zariadenia, na ktorom je spustený. TCPView slúži skorej na zistenie, či nejaké procesy na pozadí sa nepripájajú na nežiadane IP adresy. Môžeme povedať že je grafickým ekvivalentom pre program „netstat“,

ktorý je dostupný cez príkazový riadok¹² s nejakými vylepšeniami. Jedno z vylepšení je, že zobrazuje názov procesu a jeho PID, ktorý nadviazal spojenie, pokúša nadviazať spojenie alebo počúva na prichádzajúcu komunikáciu. Medzi štandardné funkcie, ktoré ponúka patrí zobrazenie lokálnej a vzdialenej IP adresy, taktiež lokálny a vzdialený port a protokol použití na komunikáciu (TCP¹³ / UDP¹⁴). Nakoniec vie zobraziť čas, kedy bola komunikácia vytvorená a počet prenesených a prijatých packetov.

4) *Process Monitor (ProcMon)*: Je to špeciálny nástroj na monitorovanie operačného systému v reálnom čase. Zachytáva podrobne udalosti týkajúce sa súborového systému, registrov a aktivity procesov, čo ho robí veľmi cenným nástrojom pri diagnostike a riešení problémov v systéme. Medzi jeho kľúčové funkcie patrí:

- **Filtrovanie udalostí:** ProcMon poskytuje robustné možnosti filtrovania, ktoré umožňujú používateľom filtrovať udalosti na základe kritérií, ako je názov procesu, cesta alebo typ operácie.
- **Sledovanie systémových volaní:** Zachytáva systémové volania, čím poskytuje náhľad na správanie aplikácií pri ich interakcii so systémovými prostriedkami Windowsu.
- **Zachytávanie krátko existujúcich procesov:** Na rozdiel od Process Explorera, Process Monitor dokáže zachytiať aj procesy, ktoré existujú len krátko, napríklad spustenie príkazu „ipconfig“ v príkazovom riadku.

Ako aj každý iný logovací nástroj, ProcMon zobrazuje čas záznamu, názov procesu, jeho PID, vykonanú operáciu (napr. čítanie z registra, zapísanie súboru a pod.), cestu k objektu, nad ktorým danú operáciu vykonal, výsledok operácie a v poslednom rade detailné informácie o operácii. Taktiež vie podobne ako Process Explorer zobraziť výpis bežiacich procesov v stromovej štruktúre s tým, že má pridaný stĺpec „lifetime“ čo zobrazuje, ako dlho proces bol spustený keď bol zapnutý nástroj ProcMon. V sekcii „Process Activity Summary“ vie nástroj zobraziť využitie systémových prostriedkov počas toho ako bol nástroj spustený. Obsahuje viacero takýchto pod-nástrojov, ktoré zobrazujú využitie prostriedkov danej kategórie, počas toho ako bol ProcMon spustený. Na záver, nástroj vie spočítať počet výskytov reťazcov z vybranej kategórie. ProcMon je teda všeobecný nástroj, na monitorovanie a analýzu operačného systému v reálnom čase. Ako hovorí Mark Russinovich, tvorca tohto nástroja: „When in doubt, run ProcMon“, čo vo voľnom preklade znamená „Ak si nie ste istí, spusťte ProcMon“.

II. POŽIADAVKY NA INŠTALÁCIU A POSTUP PRI INŠTALÁCIÍ

A. Systémové požiadavky

Systémové požiadavky na nainštalovanie balíka nástrojov Sysinternals sú v podstate rovnaké, ako na samotný operačný systém MS Windows, pretože Sysinternals podporuje všetky aktuálne verzie MS Windows. Môžeme ich vidieť v Tabuľke

⁸malvér

⁹ASEP — AutoStart Extensibility Points

¹⁰Task Scheduler

¹¹Startup application

¹²CLI — Command Line Interface

¹³TCP — Transmission Control Protocol

¹⁴UDP — User Datagram Protocol

TABUĽKA II: MINIMÁLNE SYSTÉMOVÉ POŽIADAVKY OS WINDOWS

Komponent	Minimálne požiadavky
Procesor	1 GHz alebo rýchlejší, 2+ jadrá, CPU schválené Microsoftom
Operačná pamäť (RAM)	4 GB
Úložisko	64 GB alebo viac
Firmware podpora	podpora UEFI ¹⁶ a Secure Boot ¹⁷
TPM ¹⁸	verzia 2.0 a vyššia
Grafická karta	Kompatibilná s DirectX 12 alebo vyšším, WDDM ¹⁹ 2.0 ovladač
Displej	Vysoké rozlíšenie (720p), >9" uhlopriečka, 8 bitov pre jeden farebný kanál

č. II. Podporuje aj viaceru CPU architektúru, medzi ktoré patria 64-bit, 32-bit a ARM¹⁵.

B. Stiahnutie balíka nástrojov

Balík nástrojov sa dá stiahnuť z oficiálnej webovej stránky Microsoftu. Je dostupný na adrese <https://learn.microsoft.com/en-us/sysinternals/downloads/>. Na tejto adrese vieme stiahnuť .zip súbor celého nástroja, alebo si vieme stiahnuť nami žiadane nástroje jednotlivu. Taktiež si vieme nástroj stiahnuť z obchodu aplikácií MS Store, kde budeme dostávať prípadné aktualizácie softvéru.

C. Inštalácia, spustenie a konfigurácia

Ak si balík nástrojov stiahneme z oficiálnej stránky, tak ho nemusíme inštalovať, stačí extrahovať .zip súbory, kde sa už nachádzajú spustiteľné .exe súbory. V prípade, že balík získame z obchodu MS Store, tak sa nám automaticky nainštaluje a nemusíme nič ďalej robiť. V prípade stiahnutia ho vieme spustiť ako klasický program dvojitým kliknutím alebo pomocou príkazového riadku. Ak sme ho získali z obchodu MS Store, tak ho vieme nájsť pomocou vyhľadávania medzi aplikáciami alebo v štart menu. Ďalšia konfigurácia po inštalácii nie je nutná.

III. EXPERIMENTOVANIE A OVERENIE FUNKCIONALÍT BEZPEČNOSTNÝCH NÁSTROJOV

A. Príprava na experimentovanie

Na experimentovanie som sa rozhodol použiť virtuálny stroj v cloude. Je to z toho dôvodu, že chcem spustiť reálny malvér na danom stroji a ide o bezpečnejšiu alternatívu ku spúšťaniu malvéru na lokálnej VM. Konkrétnie som si vybral cloudovú službu Linode (dnes známu ako Linode by Akamai alebo skrátene Akamai²¹) pretože pomocou promo kódu som získal 100\$ na spojazdnenie virtuálnych strojov a mal som predošlé skúsenosti s touto platformou. Kedže zámerom môjho projektu je balík nástrojov zameraný na ope-

¹⁵Advanced RISC Machines — používa sa pri procesoroch mobilných zariadení

¹⁶Unified Extensible Firmware Interface

¹⁷Zabezpečené spustenie

¹⁸Trusted Platform Module

¹⁹Windows Display Driver Model

²⁰VM — Virtual Machine

²¹Spoločnosť Akamai odkúpila spoločnosť Linode v roku 2022

račný systém Windows, potreboval som si vytvoriť virtuálny stroj na Linode. Nanešťastie Linode neposkytuje priamo na výber OS Windows, ale ponúka iba GNU+Linux distribúcie ako napríklad Ubuntu, Debian, Arch, CentOS, Fedora, Kali, Rocky a mnohé ďalšie. Našiel som však veľmi dobrý návod na to, ako spojazdniť virtuálny stroj s OS Windows na platforme Linode [3].

Krátky prehľad krokov z uvedeného návodu, ktorý poskytol samotný autor, upravený podľa mojich potrieb:

- Vytvorte dva virtuálne počítače, jeden na Linode a jeden na vašom lokálnom počítači.
- Nainštalujte systém Windows do vášho miestneho virtuálneho počítača a povolte pripojenie k vzdialej ploche.
- Naklonujte disk miestneho virtuálneho počítača na VPS²² Linode.
- Zväčšite veľkosť diskového oddielu systému Windows, aby ste zaplnili miesto na disku VPS.
- Na pripojenie k VPS použite RDP na miestnom počítači GLISH²³ (webovú grafickú konzolu) poskytovanú Linodom.

B. Experimenty s vybranými nástrojmi

Kedže nástroje sú väčšinou používané kombinovane a nie samostatne, tak som experimentoval tým spôsobom, že som mal spustené všetky nástroje naraz a následne som spustil vybraný malvér a snažil sa zistíť jeho správanie respektíve, či by ho nástroje vedeli zachytiť. Vybral som si nasledovné typy malvéru:

- Bitcoin Miner [4]
- CryptBot [5]
- Vidar Stealer [5]
- DCRat - (Dark Crystal RAT²⁴) [5]

Zvolil som si práve tieto typy malvéru, pretože z ich typov vyplýva že budú zachytiteľné danými nástrojmi, napr. Vidar Stealer sa určite bude chcieť pripojiť na nejaké cudzie IP adresy, aby odosolal ukradnuté údaje útočníkovi a podobne. Kedže zakaždým išlo o starší malvér, ktorý bol už dávno analyzovaný a zachytený, tak som musel vypnúť antivírus Windows Defender, ktorý ho detegoval a vždy ho chcel vymazať.

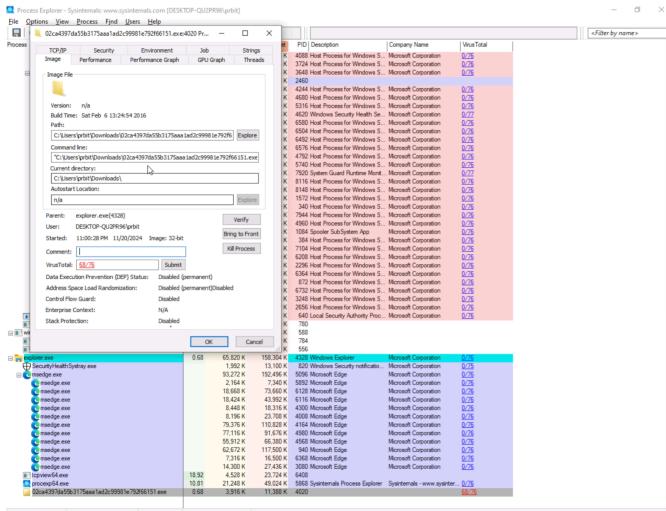
1) *Bitcoin Miner*: Stiahol som si daný malvér a extrahoval som ho pomocou aplikácie 7-zip, pretože takýto malvér určený na testovanie sa dáva do šifrovaných archívov, aby sa predišlo náhodnému spusteniu. Následne som si zapol všetky vyššie spomenuté nástroje z balíka Sysinternals a spustil som malvér. Ako prvé som sa pozrel do Process Explorera a zapol som si odosielanie vzoriek na VirusTotal. VirusTotal do pár sekúnd vrátil stav 68/76, čo znamená že 68 anti-malvérov enginov detegovalo že ide o malvér, čo môžeme vidieť na Obrázku č. 1. Ukážku priamo zo stránky VirusTotal môžeme vidieť na Obrázku č. 2. Následne som si otvoril Autoruns, kde bohužiaľ nebolo nič vidieť. Mohlo to byť z dôvodu, že malvér detegoval že sa nachádza na virtuálnom stroji a nechcel sa pri tom ako bol spustený zapísat do registrov, aby sa skryl v systéme a neboli príliš viditeľný pre bezpečnostných analytikov. Potom

²²Virtual Private Server — Virtuálny súkromný server

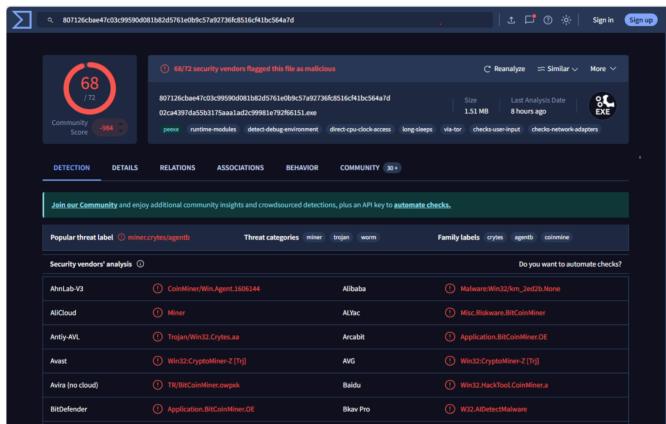
²³Graphical Linode Shell

²⁴Remote Access Trojan

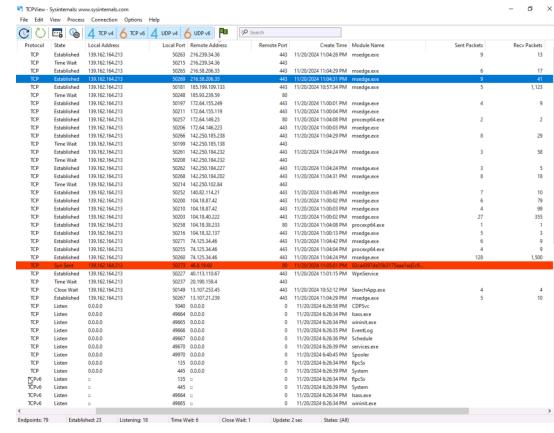
pomocou nástroja TCPView, som občas vedel zachytiť, na ktoré cudzie IP adresy sa daný malvér snaží pripojiť, čo je možné vidieť na Obrázku č. 3. Kedže ide o starší malvér tak na daných IP adresách sa už asi nič nenachádzalo a preto sa tieto spojenia po chvíli zrušili. Na záver som si otvoril už dávno spustený ProcMon, ktorý zachytával správanie malvéru od začiatku spustenia. Na Obrázku č. 4 si môžeme všimnúť, ktoré klúče z registrov používal, aké sieťové spojenia vytváral a vyznačené, sú súbory ku ktorým pristupoval respektíve ich vytváral. Následne som sa išiel pozrieť, čo sú toto za súbory. Boli to obyčajné .htm súbory (zdrojové kódy webových stránok), ktoré však boli prázdne. Môžeme ich vidieť na Obrázku č. 5. Prázdne mohli byť z dôvodu že sa malvéri nepodarilo nič stiahnuť z webu keďže vyššie spomenuté IP adresy už neboli prístupné alebo tieto súbory, ako ich meno napovedá, slúžili iba na nejaké testovanie.



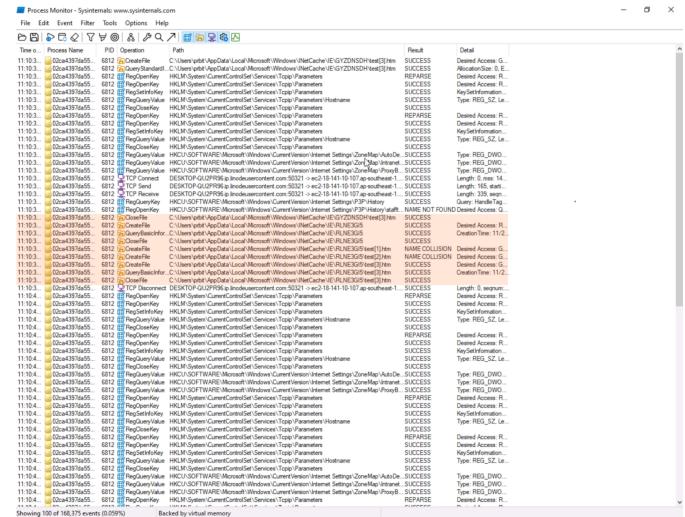
Obrázok č. 1: Bitcoin Miner — Process Explorer



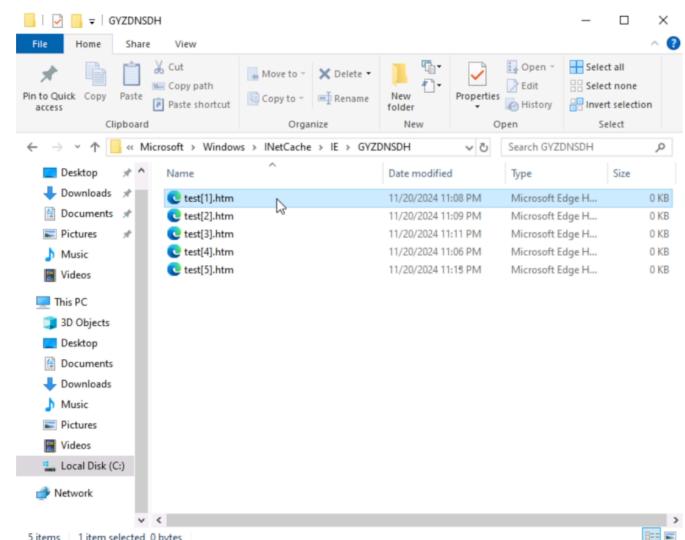
Obrázok č. 2: Bitcoin Miner — VirusTotal



Obrázok č. 3: Bitcoin Miner — TCPView

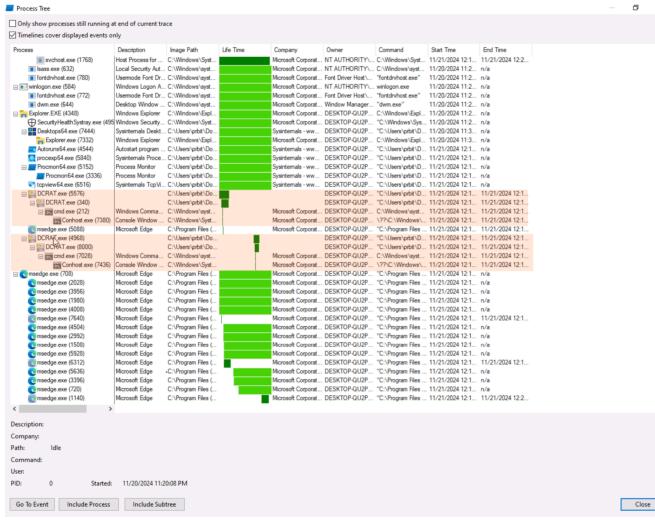


Obrázok č. 4: Bitcoin Miner — Process Monitor

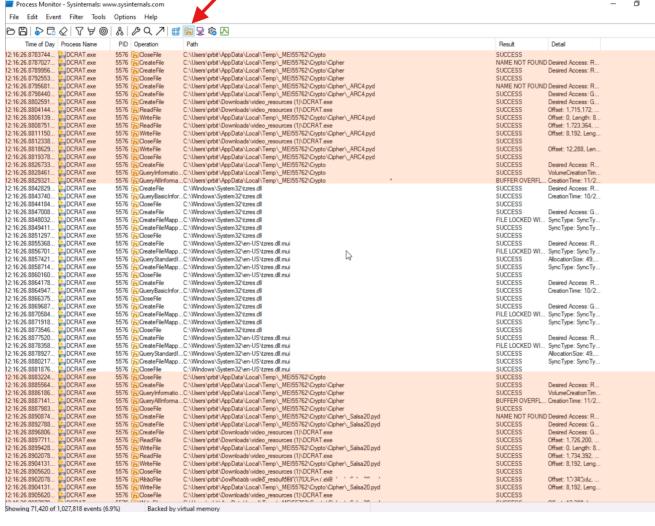


Obrázok č. 5: Bitcoin Miner — Náhodné súbory v prieskumníku

2) *CryptBot*: Pre tento malvér platil rovnaký postup ako bolo vyššie spomenuté, t.z. stiahol som si daný malvér a extrahoval som ho pomocou aplikácie 7-zip. Následne som si zapol



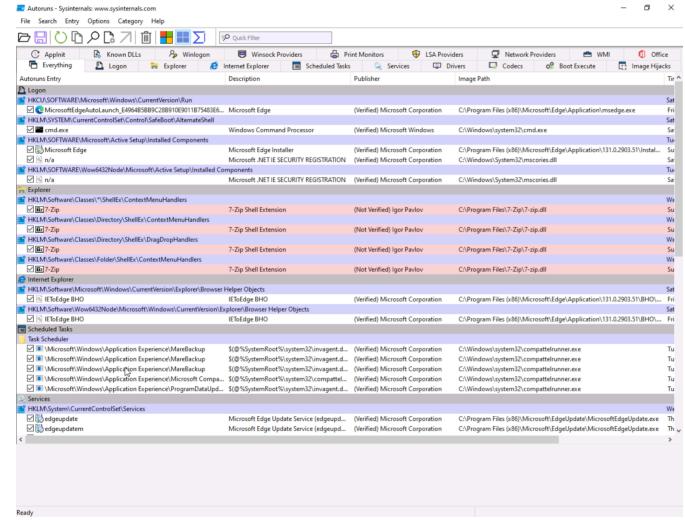
Obrázok č. 9: DCRat — ProcMon



Obrázok č. 10: DCRat — Operácie so súborovým systémom — ProcMon

C. Experiment s legitímnym softvérom

Kedže sme pomocou žiadneho malvérhu nedemonštrovali funkcionality nástroja Autoruns, rozhodol som sa že ju demonštrujem na legitímnom softvéri. Z dôvodu predchádzajúcej skúsenosti som si vybral práve 7-zip čo je nástroj na komprimáciu súborov. Kedže autor nechce platiť peniaze za certifikát, tak násntroj Autoruns udáva, že sa certifikát napriek tomu, že je program ním podpísaný nedá overiť. Túto skutočnosť si môžeme všimnúť na Obrázku č. 11. V tomto prípade, keďže ide o legitimny softvér, tak túto skutočnosť nemusíme nejakovo veľmi riešiť a taktiež VirusTotal udáva 0 identifikácií od anti-malvér enginov. Avšak v niektorých prípadoch sa malvér môže maskovať za legitimny softvér (čo aj často robí) napríklad aj za program 7-zip z čoho vyplýva, že by sme to nemali brať na ľahkú váhu.



Obrázok č. 11: Demonštrovanie nástroja Autoruns

IV. ZHODNOTELENIE BALÍKA NÁSTROJOV

Balík nástrojov Microsoft Sysinternals ponúka výbornú sadu nástrojov na vyhľadávanie a riešenie problémov spojených s malvériom a bezpečnostnými hrozbami v operačnom systéme Microsoft Windows. Programy Process Explorer, Autoruns, TCPView a Process Monitor umožňujú sledovať procesy, sieťovú aktivity a zmeny v registroch, čo pomáha lepšie pochopiť správanie podozrivých aplikácií. Tieto nástroje spolu dokážu odhaliť a analyzovať aj zložitejšie hrozby. Experimenty na rôznych vzorkách malvérhu ukázali, že sú veľmi užitočné, aj keď niektoré pokročilé druhy malvérhu sa vedia vyhnúť detekcii, najmä na virtuálnych strojoch. Celkovo je táto sada nástrojov skvelým pomocníkom pre každého, kto sa zaobera kybernetickou bezpečnosťou ale je vhodná aj pre „obyčajných“ IT technikov alebo ľudí čo majú IT ako hobby.

Poďakovanie

Chcel by som podakovať úžasnemu tímu a komunité, ktorý stojí za jazykom Typst, v ktorom bola táto práca písaná. Je výbornou a jednoduchou alternatívou jazyka LaTeX s prvkami jazyka Markdown. Veľká vďaka patrí aj ľuďom, ktorí stojí za jasnotou a zrozumiteľnosťou dokumentáciu tohto jazyka. Na záver by som chcel podakovať autorovi návodu na sprevádzkovanie Winodws 10 na Linode VPS [3] a autorom GitHub repozitárov s vzorkami malvérhu [4], [5].

LITERATÚRA

- [1] Wikipedia contributors, “Sysinternals — Wikipedia, The Free Encyclopedia”. [Online]. Available at: <https://en.wikipedia.org/w/index.php?title=Sysinternals&oldid=1248667707>
- [2] Microsoft, “Microsoft Sysinternals Documentation”. [Online]. Available at: <https://learn.microsoft.com/en-us/sysinternals/>
- [3] Scott Lott, “Installing Windows on a Linode VPS”. [Online]. Available at: <https://github.com/only-cliques/docs/blob/windows-on-linode/docs/tools-reference/windows-on-linode/installing-windows-on-linode-vps.md>
- [4] Fabrizio Monaco, “Malware Samples Repository”. [Online]. Available at: <https://github.com/fabrimagic72/malware-samples/tree/master>
- [5] Josh Stroschein, “Malware Samples Repository”. [Online]. Available at: <https://github.com/jstrosch/malware-samples>

- [6] VirusTotal contributors, “VirusTotal Documentation Hub”. [Online]. Available at: <https://docs.virustotal.com/>
- [7] Mark Russinovich, “License to Kill: Malware Hunting with the Sysinternals Tools”. [Online]. Available at: https://www.youtube.com/watch?v=A_TPZxuTzBU
- [8] Windows IT Pro, “Sysinternals Overview | Microsoft, tools, utilities, demos”. [Online]. Available at: <https://www.youtube.com/watch?v=6RqFPrCcWfY>